ZYXEL NETWORKS

www.zyxel.com

Zyxel GS1900 Series V2.60(Axxx.2)C0

Release Note

Date: Sep. 17, 2020

This document describes the features in the GS1900 series product for its V2.60(Axxx.2)C0 release.

Support Platforms:

- Zyxel GS1900-8
- Zyxel GS1900-8HP
- Zyxel GS1900-8HP (Rev. B1)
- Zyxel GS1900-8HPv2
- Zyxel GS1900-10HP
- Zyxel GS1900-16
- Zyxel GS1900-24E
- Zyxel GS1900-24EP
- Zyxel GS1900-24
- Zyxel GS1900-24HP
- Zyxel GS1900-24HPv2
- Zyxel GS1900-48
- Zyxel GS1900-48HP
- Zyxel GS1900-48HPv2

Version:

System Version	V2.60(AAHH.2) | 09/17/2020 V2.60(AAHI.2) | 09/17/2020 V2.60(AAZI.2) | 09/17/2020 V2.60(AAHJ.2) | 09/17/2020 V2.60(AAHK.2) | 09/17/2020 V2.60(AAHL.2) | 09/17/2020

	V2.60(AAHM.2) | 09/17/2020 V2.60(AAHN.2) | 09/17/2020 V2.60(AAHO.2) | 09/17/2020 V2.60(ABTO.2) | 09/17/2020 V2.60(ABTP.2) | 09/17/2020 V2.60(ABTQ.2) | 09/17/2020
Boot Version	V2.0.1.8| 06/19/2020 V2.0.0.1 | 08/14/2020

Read Me First:

GS1900-8HP Rev. B1 and GS1900-10HP only can support firmware V2.10(AAxx.0)C0 or above version.

New Features:

V2.60(Axxx.2)C0

N/A

V2.60(Axxx.1)C0

N/A

V2.60(Axxx.0)C0

1. **[LLDP]** Support LLDP "Power via MDI".
2. **[Time]** Support India time zone.
3. **[Syslog]** Support "go to designated page" in syslog page on Web GUI.

V2.50(AAxx.0)C0

N/A

V2.40(AAxx.2)C0

N/A

V2.40(AAxx.1)_20180705:

1. **[Management]** Support enable/disable Telnet and SSH.
2. **[HTTPS]** One click to regenerate certificate and extend valid period.

V2.40(AAxx.1)C0

1. **[Tech Support]** Add Tech support level log for advance trouble shooting.

Enhanced Features:

V2.60(Axxx.2)C0

N/A

V2.60(Axxx.1)C0

1. **[LED]** Synchronize the LED behavior between GS1900-48HPv1 and GS1900-48HPv2.
2. **[SSH]** Remove "disable" command from Telnet/SSH switch.
3. **[Authentication]** Enhance web user login authentication mechanism.

V2.60(Axxx.0)C0

1. **[LLDP]** Enlarge LLDP system description length to 512 bits.
2. **[DHCP]** Switch will keep requesting DHCP IP after booting up instead of staying at default IP. Once switch receives DHCP IP, it will have a log to indicate the IP has been changed from default IP to DHCP IP.

V2.50(AAxx.0)C0

1. **[SSH]** Change SSH default to disable

V2.40(AAxx.2)C0

2. eITS#180800328
   [HTTPS] Support the version of TLS to 1.2

V2.40(AAxx.1)_20180705

1. **[HTTPS]** Support SHA-2 authentication for https.

V2.40(AAxx.1)C0

1. **[Mirror]** Support Mirror CPU Traffic.

V2.40(AAxx.0)C0:

1. **[PoE]** PoE default mode changes from Classification mode to Consumption mode.
2. eITS#170200226
   [Time Range] Time range groups for PoE scheduling.
3. **[Voice VLAN]** Voice VLAN behavior enhancement (It can process the untagged packets from IP phone).
4. **[Web GUI]** Brand 2.0 GUI.
5. **[SNMP]** Firmware upgrade via SNMP.

V2.30(AAxx.0)C0:

1. eITS#161000855
   [Time] Modify Daylight Savings Time configuration for "Week" from [1,2,3,4,5] to [1,2,3,4, Last].

Bug Fixed:

V2.60(Axxx.2)C0

1. **[Vulnerability]** Fix SSH vulnerability issue.
2. eITS# 200900694/200901072
   [System] Switch will reboot unexpectedly due to SNMP memory leak.

V2.60(Axxx.1)C0

1. **[Password]** Password can't be changed from the link on warning page.
2. **[Web GUI]** Port information can't be displayed properly on virtual device.
3. **[Vulnerability]** Fix vulnerability issue for Reflected Cross Site Scripting, Stored Cross Site Scripting, Cross Site Request Forgery.

Vulnerable conditions apply only if the administrator has logged in the switch by the web interface and active session is maintained, whilst the attack also requires knowledge of the private IP of the switch.

V2.60(Axxx.0)C0:

1. eITS#200200818
   [Web GUI] Correct wording on Web GUI.
2. eITS#200107081
   [LAG] Fix inconsistency of LAG VLAN setting between V2.50 and V2.40
3. eITS#191101097
   [Syslog] Fix QoS syslog display error.
4. **[Voice VLAN]** Fix Voice VLAN is always tagged out even if the port is configured as untagged.

V2.50(AAxx.0)C0:

1. **[Vulnerability]** Fix vulnerability issue for CVE-2019-11478.
2. **[Vulnerability]** Fix vulnerability issue for CVE-2019-11479.
3. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15799.
4. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15800.
5. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15801.
6. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15802.
7. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15803.
8. **[Vulnerability]** Fix vulnerability issue for CVE-2019-15804.
9. **[Vulnerability]** Fix vulnerability issue for SSH authentication mechanism. Upon connection, the SSH session will be established and allows for tunneling.

V2.40(AAxx.2)C0:

1. eITS#180500245
   [Web GUI] The switch automatically redirects the IPv6 page to IPv4 after rebooting switch.
2. eITS#180700932

[Web GUI] VLAN Wizard screen doesn't resize correctly, it can only shows first 30 ports.

3. eITS#180600290
   [IGMP] Memory leak in the multicast module caused the switch to reboot.
4. **[Web GUI]** Web GUI doesn't display correctly when using Safari browser.
5. eITS#181000519
   [Web GUI] Web GUI doesn't display properly if the resolution is above 2560X1440.
6. eITS#181000729
   [LLDP] Switch unable to recognize LLDP packet from HP switch.
7. eITS#181100948
   [System] Switch can be configured via CLI if logged into switch by telnet/ssh then input command "traceroute ;/bin/cli", after re-login switch, configure terminal can be accessed.
8. **[Tech-support]** The port number of mac address table does not appear on Tech-support.
9. **[Vulnerability]** Multiple buffer overflow vulnerabilities were identified in embedded web server with several improper usage of "strcpy()" calls while processing the web requests; and the device's web-server returns the HTTP 'ETag' header with specific value that could allow remote fingerprinting of the device.

V2.40(AAxx.1)_20180705:

1. **[Vulnerability]** Vulnerability issue: NVT: TESO in.telnetd buffer overflow.
2. **[Vulnerability]** Vulnerability issue: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS.
3. **[Vulnerability]** Vulnerability issue: SSL/TLS: Report Weak Cipher Suites.
4. **[Vulnerability]** Vulnerability issue: TCP timestamps Mitigation.
5. eITS#180501059
   [SNMP] ifInError MIB counter changes abnormally under FreeBSD system.

V2.40(AAxx.1)C0:

1. eITS#180300318/ 180300320
   [System] Since FW v2.10, GS1900-8 may sometimes have unexpected random reboot under some network application.
2. eITS#180200590
   [Syslog] The new syslog messages can't be record due to its buffer is full and can't be overwritten.

V2.40(AAxx.0)C0:

1. eITS#170500544
   [DHCP] Change management VLAN does not trigger device's DHCP client to renew IP address.
2. eITS#170100069
   [VLAN] VLAN 1's name cannot be saved after rebooting.
3. **[SNMP]** When using SNMPc tool to reboot switch will pop-up error message, but switch will reboot successful.
4. eITS#170600306
   [Web GUI] The switch automatically redirects the IPv6 page to IPv4 after IPv6 session time-out.
5. eITS#170700123
   [IPv6] The switch automatically redirects the Link-local IPv6 address to global IPv6 address after session time-out.
6. eITS#170700205
   [Management] User may download the running configuration with a particular method without authentication.
7. eITS#170900867
   [Time Range] The "Time Range" can neither be edited nor be deleted if the user set the Time Range Name with "space".
8. eITS#170900256
   [SNMP] When polling some particular SNMP OID that may causes device in high memory usage and loss of the management.
9. eITS#171000804

[IGMP] GS1900-8HP/24E does not send specific IGMPv3 report across uplink port.

10. **[Web GUI]** Login page's system name characters will over the border when system name is set to 64 characters.

V2.30(AAxx.0)C0:

1. eITS#161000065
   [STP] Spanning Tree Forward Delay parameter reverts back to 15 seconds after saving and rebooting the switch.
2. eITS#161000488
   [Web GUI] Mozilla Firefox version 49.0.1 cannot view some characters in GS1900 web GUI.
3. eITS#161000852
   [NTP] GS1900 cannot sync with time server if time server is configured using DNS.
4. eITS#161000847
   [LAG] LACP cannot work with the accept frame type as "tagged only".
5. **[SNMP]** Sometimes set name will failure via SNMP.
6. **[LLDP]** When receive the too long LLDP-MED Hardware version packets will cause switch hang up.

V2.20(AAxx.1)C0:

1. **[PoE]** Switch PoE LED button is abnormal.

V2.20(AAxx.0)C0:

1. eITS#160400893
   [System] Syslog time stamp inconsistent with system time.
2. eITS#160301255
   [LAG] LACP does not timeout in 3 seconds when using LACP "1 second" interval.
3. eITS#160401062
   [Config] Cannot remove the port of link aggregation from Web Wizard.
4. eITS#160600848

[Port security] Configure "Max MAC Entry Number" to "0" and it changes to "1" automatically after reboot.

5. eITS#160200029
   [LAG] Sometimes LACP trunk will fail for 4 minutes.
6. **[Vulnerability]** Fix for CVE-2016-0800.

Known Issue:

1. **[Logging]** If user tries to restore an illegal configuration (unofficial), login will always show authentication fail.
2. **[Web GUI]** System name display incorrect when using the special characters.
3. **[Web GUI]** Some pages cannot display correct when IE 8 enable "Compatibility View Settings".
   [Workaround] Upgrade IE browser to the latest version or disable "Compatibility View Settings."
4. **[Firmware]** Downgrade from V2.50 to V2.40 and below versions will cause admin account unable to login. This is due to password authentication algorithms are enhanced for vulnerability issues and is not backwards compatible.
   In the unlikely event of downgrading firmware, resetting to default can then login with default account and password.
5. **[Firmware]** Switch firmware V2.50 is only compatible with ZON V2.1.4, ZON V2.1.3 and lower are not compatible. Functions requiring password authentication will fail to authenticate due to previous ZON version does not support V2.50 password authentication algorithms.

Limitations:

1. 802.1s instances : 16
2. Guest VLAN : 1

3. Static MAC entries : 64
4. The BWM works well with UDP only.

Change History:

- V2.60(Axxx.2) | 09/17/2020
- V2.60(Axxx.1) | 06/17/2020
- V2.60(Axxx.0) | 02/25/2020
- V2.50(AAxx.0) | 10/21/2019
- V2.40(AAxx.2) | 06/05/2019
- V2.40(AAxx.1)_20180705 | 07/05/2018
- V2.40(AAxx.1) | 03/30/2018
- V2.40(AAxx.0) | 11/07/2016
- V2.30(AAxx.0) | 12/14/2016
- V2.20(AAxx.1) | 09/02/2016
- V2.20(AAxx.0) | 06/23/2016
- V2.10(AAxx.0) | 09/10/2015
- V2.00(AAxx.2) | 02/09/2015
- V2.00(AAxx.1) | 10/20/2014
- V2.00(AAxx.0) | 06/25/2014
- V1.00(AAxx.0) | 07/24/2013